What is claimed is:

1. A method of digitally fingerprinting authorized video signals comprising the steps of:

producing signals with spatial frequencies selected by a crypto graphically secure random number generator; and

adding the signals to the chroma data of the video signal using components of a rotating complex exponential;

whereby the signals identify the original source of the authorized video signal and thereby enable criminal prosecution of parties responsible for unauthorized duplication of the video signal.

2. The method of claim 1 further comprising the step of controlling the random number generator with a key that is unique to the video signal to be watermarked.

3. The method of claim 1 further comprising the step of inputting a time code representative of the elapsed time of the video signal into the random number generator.

4. The method of claim 1 further comprising the step of crypto graphically deriving binary information from the video signal for keying the spatial frequencies on and off.

5. The method of claim 1 wherein the signals are added by perceptually significant chroma data at low intensity.

6. The method of claim 1 wherein the signals are added by chroma data and the method further comprises the step of preserving the chroma data by common compression algorithms.

7. The method of claim 1 further comprising the step of recovering the signals by subtracting the chroma data of a suspected unauthorized copy of the video signal from the chroma data of the authorized video signal.

8. The method of claim 7 further comprising the step of transforming the authorized video signal.

9. The method of claim 8 wherein the authorized video signal is transformed by the same algorithm or algorithms as the suspected unauthorized copy of the video signal.

10. The method of claim 7 further comprising the step of accumulating recovered signals from frame to frame.

11. The method of claim 7 further comprising the step of detecting the presence or absence of spectral components in the recovered signals by phase coherent demodulation at the selected spatial frequencies.

12. The method of claim 11 further comprising the step of accumulating recovered signals from frame to frame.

13. The method of claim 12 further comprising the step of interpreting the presence or absence of spectral components in the recovered signals to identify the authorized video signals from which the suspected unauthorized copy of the video signal was created.

14. The method of claim 13 wherein the step of interpreting provides a high probability of identifying any unauthorized copies of the

authorized video signal and a negligible probability of identifying an authorized video signal which was not copied.

15. The method of claim 7 further comprising the step of detecting the presence or absence of spectral components in the recovered signals by phase incoherent demodulation at the selected spatial frequencies.

16. The method of claim 15 further comprising the step of accumulating recovered signals from frame to frame.

17. The method of claim 16 further comprising the step of interpreting the presence or absence of spectral components in the recovered signals to identify the authorized video signals from which the suspected unauthorized copy of the video signal was created.

18. The method of claim 17 wherein the step of interpreting provides a high probability of identifying any unauthorized copies of the authorized video signal and a negligible probability of identifying an authorized video signal which was not copied.

19. The method of claim 7 further comprising the step of detecting the presence or absence of spectral components in the recovered signals by phase incoherent demodulation at the selected spatial frequencies.

20. The method of claim 9 further comprising the step of detecting the presence or absence of spectral components in the recovered signals by phase incoherent demodulation at the selected spatial frequencies.

21. A method of digitally fingerprinting authorized video signals comprising the steps of:

producing signals with spatial frequencies selected by a crypto graphically secure random number generator; and

adding the signals to the intensity data of the video signal using components of a rotating complex exponential;

whereby the signals identify the original source of the authorized video signal and thereby enable criminal prosecution of parties responsible for unauthorized duplication of the video signal.

22. The method of claim 21 further comprising the step of recovering the signals by subtracting the intensity data of a suspected unauthorized copy of the video signal from the intensity data of the authorized video signal.

23. A method of digitally fingerprinting authorized video signals comprising the steps of:

deriving a unique key from the authorized video signal;

inputting the key into a crypto graphically secure random number generator;

controlling the random number generator with the key to produce signals with spatial frequencies; and

adding the signals to a portion of the authorized video signal using components of a rotating complex exponential;

whereby the signals identify the original source of the authorized video signal and thereby enable criminal prosecution of parties responsible for unauthorized duplication of the video signal.